(19)日本国特許庁（ＪＰ）　(12) **公表特許公報（Ａ）**　(11)特許出願公表番号
特表2002－514326
（P2002－514326A）
(43)公表日　平成14年５月14日(2002.5.14)

(51)Int.Cl.[7]	識別記号	Ｆ Ｉ		テーマコード（参考）
Ｇ０６Ｆ　11/00		Ｇ０６Ｆ　13/00	５３０Ａ	
13/00	５３０	9/06	６６０Ｎ	

審査請求　未請求　　予備審査請求　有　　（全 38 頁）

(21)出願番号　特願平10－522345
(86)（22)出願日　平成９年11月６日(1997.11.6)
(85)翻訳文提出日　平成11年５月８日(1999.5.8)
(86)国際出願番号　ＰＣＴ／ＩＢ９７／０１６２６
(87)国際公開番号　ＷＯ９８／２１６８３
(87)国際公開日　平成10年５月22日(1998.5.22)
(31)優先権主張番号　６０／０３０，６３９
(32)優先日　平成８年11月８日(1996.11.8)
(33)優先権主張国　米国（ＵＳ）
(31)優先権主張番号　０８／９６４，３８８
(32)優先日　平成９年11月６日(1997.11.6)
(33)優先権主張国　米国（ＵＳ）

(71)出願人　フィンジャン　ソフトウェア，リミテッド
イスラエル国，42945　ケファー・ハイム
(72)発明者　トウボウル，シュロモ
イスラエル国，42945　ケファー・ハイム
(74)代理人　弁理士　飯塚　義仁

最終頁に続く

(54)【発明の名称】　悪意のあるダウンローダブルからコンピュータおよびネットワークを保護するためのシステムおよび方法

(57)【要約】
システムは、疑わしいダウンローダブルからコンピュータを保護する。このシステムは、セキュリティポリシーと、ダウンローダブルを受け取るためのインターフェイスと、このインターフェイスに接続されていて、前記セキュリティポリシーを前記ダウンローダブルに適用して、前記セキュリティポリシーが侵害されたか否かを判定するためのコンパレータとを備えている。前記ダウンローダブルは、Java（商標）アプレット、ActiveX(商標)コントロール、JavaScript(商標)スクリプト、または、Visual Basicスクリプトを含んでいてよい。前記セキュリティポリシーは、前記ダウンローダブルの宛先であるクライアントに関わらず適用されるデフォルトセキュリティポリシー、前記クライアントまたは該クライアントが属するグループに基づいて適用される特定のセキュリティポリシー、または、前記クライアント／グループおよび受け取った特定のダウンローダブルに基づいて適用される特定のセキュリティポリシーを含んでいてよい。このシステムは、好ましくは、前記ダウンローダブルのすべての構成要素をフェッチし、このフェッチした

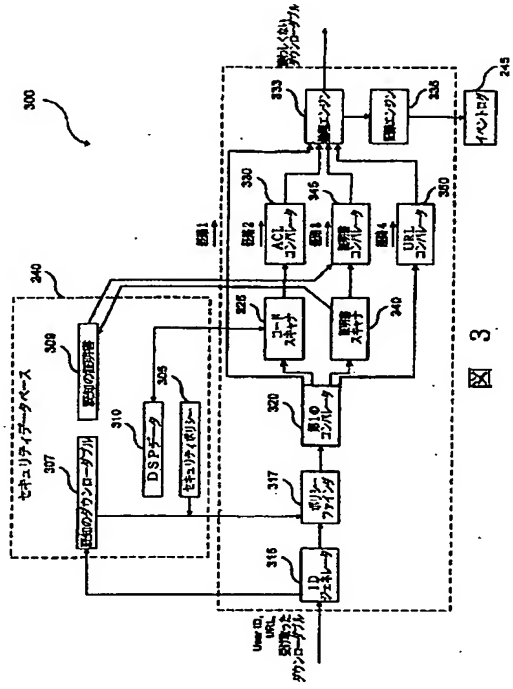

図３

【特許請求の範囲】

１．ダウンローダブルを受け取るステップと、

前記ダウンローダブルをセキュリティポリシーと比較し、前記セキュリティポリシーが侵害されたか否かを判定するステップと、

前記セキュリティポリシーが侵害された場合、前記ダウンローダブルを放棄するステップと

を具備するコンピュータに基づく方法。

２．前記ダウンローダブルをダウンローダブルセキュリティファイルに分解するステップと、該ダウンローダブルセキュリティファイルを前記セキュリティポリシーと比較するステップとをさらに具備した請求の範囲第１項に記載の方法。

３．証明書をスキャンし、該証明書を信頼性が確認された証明書と比較するステップをさらに具備した請求の範囲第１項に記載の方法。

４．前記ダウンローダブルの送り元のＵＲＬを既知のＵＲＬと比較するステップをさらに具備した請求の範囲第１項に記載の方法。

５．前記既知のＵＲＬが信頼性が確認されたＵＲＬである請求の範囲第４項に記載の方法。

６．前記既知のＵＲＬが信頼性が確認されていないＵＲＬである請求の範囲第４項に記載の方法。

７．前記ダウンローダブルがJava（商標）アプレットを含む請求の範囲第１項に記載の方法。

８．前記ダウンローダブルがActiveX（商標）コントロールを含む請求の範囲第

１項に記載の方法。

９．前記ダウンローダブルがJavaScript（商標）スクリプトを含む請求の範囲第１項に記載の方法。

１０．前記ダウンローダブルがVisual Basicスクリプトを含む請求の範囲第１項に記載の方法。

１１．前記ダウンローダブルの宛先がクライアントであり、前記セキュリティポリシーは、前記ダウンローダブルの宛先であるクライアントにかかわらず適用さ

れるデフォルトセキュリティポリシーを含む請求の範囲第１項に記載の方法。

１２．前記ダウンローダブルの宛先がクライアントであり、前記セキュリティポリシーは、前記ダウンローダブルの宛先がクライアントである場合に適用される特定のセキュリティポリシーを含む請求の範囲第１項に記載の方法。

１３．前記ダウンローダブルの宛先がグループに属するクライアントであり、前記セキュリティポリシーは、前記クライアントが特定のグループに属する場合に適用される特定のセキュリティポリシーを含む請求の範囲第１項に記載の方法。

１４．前記ダウンローダブルの宛先がクライアントであり、前記ダウンローダブルを放棄した後に、その代替となる悪意の無いダウンローダブルを前記クライアントに送って通知するステップをさらに具備した請求の範囲第１項に記載の方法。

１５．前記ダウンローダブルを放棄した後に、前記侵害をイベントログに記録するステップをさらに具備した請求の範囲第１項に記載の方法。

１６．前記ダウンローダブルを識別するためのダウンローダブルＩＤを算出するステップをさらに具備した請求の範囲第１項に記載の方法。

１７．前記ダウンローダブルによって特定される構成要素をフェッチし、該フェッチされた構成要素を前記ダウンローダブルに含めるステップをさらに具備した請求の範囲第１６項に記載の方法。

１８．前記ダウンローダブルについてハッシング関数を実行するステップをさらに具備した請求の範囲第１７項に記載の方法。

１９．前記ダウンローダブルによって特定されるすべての構成要素をフェッチするステップをさらに具備した請求の範囲第１７項に記載の方法。

２０．意図された受領者のユーザＩＤを検査し、適当なセキュリティポリシーを決定するステップをさらに具備した請求の範囲第１項に記載の方法。

２１．前記ダウンローダブルを検査し、適当なセキュリティポリシーを決定するステップをさらに具備した請求の範囲第１項に記載の方法。

２２．前記適当なセキュリティポリシーが、デフォルトセキュリティポリシーを含む請求の範囲第２０項に記載の方法。

２３．前に受け取ったダウンローダブルを既知のダウンローダブルとして含めるステップをさらに具備した請求の範囲第２６項に記載の方法。

２４．前記セキュリテイポリシーが、管理オーバーライドごとに拒絶すべきダウンローダブルを指示する請求の範囲第２３項に記載の方法。

２５．前記セキュリティポリシーが、管理オーバーライドごとに許可すべきダウンローダブルを指示する請求の範囲第２３項に記載の方法。

２６．前記ダウンローダブルを既知のダウンローダブルと比較するステップをさらに具備した請求の範囲第１項に記載の方法。

２７．前記既知のダウンローダブルが悪意のあるものである請求の範囲第２６項に記載の方法。

２８．前記既知のダウンローダブルが悪意の無いものである請求の範囲第２６項に記載の方法。

２９．前記セキュリティポリシーがアクセスコントロールリストを含み、前記ダウンローダブルのセキュリティプロファイルデータを前記アクセスコントロールリストと比較するステップをさらに具備した請求の範囲第２項に記載の方法。

３０．セキュリティポリシーの侵害を検出したときに、ユーザに通知するステップをさらに具備した請求の範囲第１項に記載の方法。

３１．セキュリティポリシーと、

ダウンローダブルを受け取るためのインターフェイスと、

前記インターフェイスに接続されていて、前記セキュリティポリシーを前記ダウンローダブルに適用して、前記セキュリティポリシーが侵害されたか否かを判定するコンパレータと

を具備したシステム。

３２．前記ダウンローダブルがJava（商標）アプレットを含む請求の範囲第３１項に記載のシステム。

３３．前記ダウンローダブルがActiveX（商標）コントロールを含む請求の範囲第３１項に記載のシステム。

３４．前記ダウンローダブルがJavaScript（商標）スクリプトを含む請求の範囲第３１項に記載のシステム。

３５．前記ダウンローダブルがVisual Basicスクリプトを含む請求の範囲第３１項に記載のシステム。

３６．前記ダウンローダブルの宛先がクライアントであり、前記セキュリティポリシーは、前記ダウンローダブルの宛先であるクライアントにかかわらず適用されるデフォルトセキュリティポリシーを含む請求の範囲第３１項に記載のシステム。

３７．前記ダウンローダブルの宛先がクライアントであり、前記セキュリティポリシーは、前記ダウンローダブルの宛先がクライアントである場合に適用される特定のセキュリティポリシーを含む請求の範囲第３１項に記載のシステム。

３８．前記ダウンローダブルの宛先がグループに属するクライアントであり、前記セキュリティポリシーは、前記クライアントが特定のグループに属する場合に適用される特定のセキュリティポリシーを含む請求の範囲第３１項に記載のシステム。

３９．前記インターフェイスに接続されていて、前記ダウンローダブルを割りするダウンローダブルＩＤを算出するためのＩＤジェネレータをさらに具備した請求の範囲第３１項に記載のシステム。

４０．前記ＩＤジェネレータが、前記ダウンローダブルのすべての構成要素を予めフェッチし、該すべての構成要素を使用して前記ダウンローダブルＩＤを算出する請求の範囲第３９項に記載のシステム。

４１．前記ＩＤジェネレータが、予めフェッチされた前記すべての構成要素のディジタルハッシュを算出する請求の範囲第４０項に記載のシステム。

４２．前記セキュリティポリシーを見つけるためのポリシーファインダをさらに具備した請求の範囲第３１項に記載のシステム。

４３．前記ポリシーファインダが、前記ユーザに基づいて前記セキュリティポリシーを見つける請求の範囲第４２項に記載のシステム。

４４．前記ポリシーファインダが、前記ユーザおよびダウンローダブルに基づい

て前記セキュリティポリシーを見つける請求の範囲第４２項に記載のシステム。

４５．前記ポリシーファインダが、前記デフォルトセキュリティポリシーを求める請求の範囲第４２項に記載のシステム。

４６．前記コンパレータが、前記セキュリティポリシーを検査して、適用すべきテストを決定する請求の範囲第３１項に記載のシステム。

４７．前記コンパレータが、前記ダウンローダブルを既知のダウンローダブルと比較する請求の範囲第４６項に記載のシステム。

４８．前記既知のダウンローダブルが悪意のあるものである請求の範囲第４７項に記載のシステム。

４９．前記既知のダウンローダブルが悪意の無いものである請求の範囲第４７項に記載のシステム。

５０．前記セキュリティポリシーが、管理オーバーライドごとに拒絶すべきダウンローダブルを指示する請求の範囲第３１項に記載のシステム。

５１．前記セキュリティポリシーが、管理オーバーライドごとに許可すべきダウンローダブルを指示する請求の範囲第３１項に記載のシステム。

５２．前記ダウンローダブルの宛先がクライアントであり、

前記コンパレータは、代替となる悪意の無いダウンローダブルを前記クライアントに送って通知する請求の範囲第３１項に記載のシステム。

５３．前記コンパレータに接続されていて、前記ダウンローダブルをダウンローダブルセキュリティプロファイルデータに分解するコードスキャナをさらに具備した請求の範囲第３１項に記載のシステム。

５４．前記コードスキャナに接続されていて、前記ダウンローダブルセキュリティプロファイルデータをアクセスコントロールリストと比較するＡＣＬコンパレータをさらに具備した請求の範囲第５３項に記載のシステム。

５５．前記コンパレータに接続されていて、前記ダウンローダブルにおける証明書を検査する証明書スキャナをさらに具備した請求の範囲第３１項に記載のシステム。

５６．前記証明書スキャナに接続されていて、前記証明書を信頼性が確認された

証明書と比較する証明書コンパレータをさらに具備した請求の範囲第５５項に記載のシステム。

５７．前記コンパレータに接続されていて、前記ダウンローダブルの送り元のＵＲＬを既知のＵＲＬと比較するＵＲＬコンパレータをさらに具備した請求の範囲第３１項に記載のシステム。

５８．前記既知のＵＲＬが信頼性が確認されていないＵＲＬである請求の範囲第５７項に記載のシステム。

５９．前記既知のＵＲＬが信頼性が確認されたＵＲＬである請求の範囲第５７項に記載のシステム。

６０．前記比較の結果に応答するための論理エンジンをさらに具備した請求の範囲第３１項に記載のシステム。

６１．前記論理エンジンが、前記セキュリティポリシーに従って応答する請求の範囲第３１項に記載のシステム。

６２．前記コンパレータに接続されていて、その結果をイベントログに記録する記録エンジンをさらに具備した請求の範囲第３１項に記載のシステム。

６３．ダウンローダブルを受け取る手段と、

前記ダウンローダブルをセキュリティポリシーと比較し、前記セキュリティポリシーが侵害されたか否かを判定する手段と、

前記セキュリティポリシーが侵害された場合、前記ダウンローダブルを放棄する手段と

を具備したシステム。

６４．ダウンローダブルを受け取るステップと、

前記ダウンローダブルをセキュリティポリシーと比較し、前記セキュリティポリシーが侵害されたか否かを判定するステップと、

前記セキュリティポリシーが侵害された場合、前記ダウンローダブルを放棄するステップと

をコンピュータに実行させるためのプログラムコードを格納してなる、コンピュータにより読み取り可能な記憶媒体。

６５．ダウンローダブルを識別するためのダウンローダブルＩＤを生成するため

のコンピュータに基づく方法であって、

ダウンローダブルコードを選択するステップと、

選択された前記ダウンローダブルコードについての関数を実行し、ダウンローダブルＩＤを生成するステップと、

前記ダウンローダブルＩＤを記憶するステップと

を具備する方法。

６６．前記関数がハッシング関数を含む請求の範囲第６５項に記載の方法。

６７．前記ダウンローダブルコードが、ダウンローダブルの構成要素に対する参照を含み、前記構成要素をフェッチするステップをさらに具備した請求の範囲第６５項に記載の方法。

６８．前記構成要素が、前記ダウンローダブルコードによって参照される第１の構成要素を含む請求の範囲第６７項に記載の方法。

６９．前記選択されたダウンローダブルコードが、前記ダウンローダブルに含まれ且つ該ダウンローダブルによって識別されるコードのすべてを含む請求の範囲第６５項に記載の方法。

７０．前記ダウンローダブルによって参照されるすべての構成要素をフェッチするステップをさらに具備した請求の範囲第６７項に記載の方法。

【発明の詳細な説明】

悪意のあるダウンローダブルからコンピュータおよびネットワークを保護するためのシステムおよび方法

発明の背景

１．発明の分野

この発明は、コンピュータネットワークに関し、特に、悪意のあるダウンローダブルからコンピュータおよびネットワークを保護するためのシステムおよび方法に関する。

２．背景技術の説明

現在のインターネットは、政府、大学、非営利団体および会社によって所有される１０万個以上の個々のコンピュータネットワークの集合であり、加速度的に拡張している。インターネットは公開的なものであるので、該インターネットは、通常“ウィルス”と呼ばれる、多くのシステムに損害を与えたりこれらを破壊したりするアプリケーションプログラムの主要発生源となっている。

従って、プログラマたちは、このようなウィルスが個々のコンピュータおよびネットワークを攻撃することを阻止するためのコンピュータおよびコンピュータネットワークセキュリティシステムを設計し続けている。ほとんどの場合、このようなセキュリティシステムは比較的成功している。しかしながら、これらのセキュリティシステムは、“ダウンローダブル(Down loadab les)”と通称されているダウンロード可能なアプリケーションプログラムに付加され、または、ダウンロード可能なアプリケーションプログラムとして構成されたコンピュータビールスを認識できるよう構成されていない。前記ダウンローダブルとは、ソースコンピュータからダウンロードされ、送り先(デスティネーション)コンピュータ上で実行される実行可能なアプリケーションプログラムである。ダウンローダブルは、典型的には、インターネットブラウザまたはウェブエンジンなどを介して、進行中の処理によってリクエストされる。ダウンローダブルの例としては、Sun Microsystems, Inc. によって開発されたJava（商標）配信環境での使用のために設計

されたJava（商標）アプレット、同じくSun Microsystems, Inc.によって開発されたJavaScriptスクリプト、Microsoft Corporationによって開発されたActiveX（商標）配信環境での使用のために設計されたActiveX(商標)コントロール、および、同じくMicrosoft Corporationによって開発されたVisual Basicが含まれる。従って、悪意のあるダウンローダブルからネットワークを保護するためのシステムおよび方法が必要となっている。

発明の要点

この発明は、疑わしいダウンローダブルからネットワークを保護するためのシステムを提供する。該システムは、セキュリティポリシー（security policy）と、ダウンローダブルを受け取るためのインターフェイスと、該インターフェイスに接続されていて、前記セキュリティポリシーを前記ダウンローダブルに適用して、前記セキュリティポリシーが侵害されたか否かを判定するためのコンパレータとを具備している。前記ダウンローダブルは、Java（商標）アプレット、ActiveX(商標)コントロール、JavaScript(商標)スクリプト、または、Visual Basicスクリプトを含んでいてよい。前記セキュリティポリシーは、前記ダウンローダブルの宛先であるクライアントに関わらず適用されるデフォルトセキュリティポリシー、前記クライアントまたは該クライアントが属するグループに基づいて適用される特定のセキュリティポリシー、または、前記クライアント／グループおよび受け取った特定のダウンローダブルに基づいて適用される特定のセキュリティポリシーを含んでいてよい。該システムは、好ましくは、前記ダウンローダブルのすべての構成要素をフェッチし、該フェッチした構成要素を含むダウンローダブルについてハッシングファンクション（hashing function；ハッシング関数）を実行することによって、前記ダウンローダブルを識別するダウンローダブルＩＤを算出するためのＩＤジェネレータを使用する。

さらに、前記セキュリティポリシーは、（１）既知の悪意のあるダウンローダブルと悪意の無いダウンローダブルとの比較、（２）管理オーバーライドごとの拒絶または許可すべきダウンローダブルの比較、（３）ダウンローダブルセキュリティプロファイルデータの、アクセスコントロールリストに対する比較、（４）前記ダウンローダブルに含まれるサーティフィケート（certificate;証明又は

証明書；以下「証明書」という）の、信頼性が確認されたサーティフィケート（certificate；証明書）に対する比較、（５）前記ダウンローダブルの送り元のＵＲＬの、信頼性が確認されたＵＲＬおよび信頼性が確認されていないＵＲＬに対する比較、を含むいくつかの実行すべきテストを指示するものであってよい。

これらのテストに基づき、論理エンジンは、前記ダウンローダブルを許可または拒絶すべきことを判定することができる。

さらに、この発明は、疑わしきダウンローダブルからコンピュータを保護するための方法を提供する。この方法は、ダウンローダブルを受け取るステップと、前記ダウンローダブルをセキュリティポリシーと比較し、前記セキュリティポリシーが侵害されたか否かを判定するステップと、前記セキュリティポリシーが侵害されたか場合、前記ダウンローダブルを放棄するステップとを具備するものである。

この発明に係るシステムおよび方法は、既知の悪意のあるダウンローダブルからコンピュータを保護するものであってよい。この発明に係るシステムおよび方法は、疑わしいと判断されるオペレーションを実行するダウンローダブルを識別することができる。該システムおよび方法は、前記ダウンローダブルのコードを検査して、該コードが疑わしいオペレーションを含むか否かを判定し、この判定に応じて前記ダウンローダブルを許可または拒絶するものとすることができる。

図面の簡単な説明

図１は、この発明に係るネットワークシステムを示すブロック図。

図２は、図１の内部ネットワークセキュリティシステムの詳細を示すブロック図。

図３は、図２のセキュリティプログラムおよびセキュリティデータベースの詳細を示すブロック図。

図４は、図３のセキュリティポリシーの詳細を示すブロック図。

図５は、図１のセキュリティ管理コンソールの詳細を示すブロック図

図６Ａは、この発明に従って、疑わしいダウンローダブルの検査を行うための方法を示すフローチャート。

図６Ｂは、図６Ａの適当なセキュリティポリシーを見つけるためのステップの詳細を示すフローチャート。

図６Ｃは、入ってくるダウンローダブルを疑わしき物と判断すべきか否かを判定するための方法を示すフローチャート。

図７は、図６におけるダウンローダブルを分解するためのステップの詳細を示すフローチャート。

図８は、ダウンローダブルを識別するためのダウンローダブルＩＤを生成するための方法８００を示すフローチャート。

好ましい実施の形態の詳細な説明

図１は、この発明に係るネットワークシステム１００を示すブロック図である。該ネットワークシステム１００は、通信チャンネル１２５を介して内部ネットワークセキュリティシステム１１０に接続された、例えば、インターネットと通称されている広域ネットワーク(ＷＡＮ)のような外部コンピュータネットワーク１０５を含んでいる。さらに、前記ネットワークシステム１００は、通信チャンネル１３０を介して前記内部ネットワークセキュリティシステム１１０に接続され、且つ、通信チャンネル１３５を介してセキュリティ管理コンソール１２０に接続された，例えば、法人のローカルエリアネットワーク(ＬＡＮ)のような内部コンピュータネットワーク１１５を含んでいる。

前記内部ネットワークセキュリティシステム１１０は、前記外部コンピュータネットワーク１０５から受け取ったダウンローダブルを検査し、疑わしいと思われるダウンローダブルが前記内部コンピュータネットワーク１１５に進入するのを阻止する。この場合、望ましくないオペレーションを行いもしくはその可能性のあるダウンローダブル、または、前記内部コンピュータネットワーク１１５の完全性に脅威を与えもしくはその可能性のあるダウンローダブルが疑わしいものと判断される。なお、“疑わしい”という用語は、悪意のある、潜在的に悪意のある、望ましくない、または、潜在的に望ましくない等々を意味する。前記セキュリティ管理コンソール１２０は、前記内部ネットワークセキュリティシステム１１０の目視確認、変更および環境設定を可能にする。

図２は、前記内部ネットワークセキュリティシステム１１０の詳細を示すブロック図である。該内部ネットワークセキュリティシステム１１０は、信号バス２２０に接続された、例えば、Intel Pentium(登録商標)マイクロプロセッサまたはMotorola Power PC(登録商標)のような中央処理ユニット（ＣＰＵ）２０５を備えている。さらに、前記内部ネットワークセキュリティシステム１１０は、前記外部コンピュータネットワーク１０５からダウンローダブルを受け取るために前記通信チャンネル１２５と信号バス２２０との間に接続された外部通信インターフェイス２１０と、疑わしいと思われないダウンローダブルを前記内部コンピュータネットワーク１１５に送るために前記信号バス２２０と前記通信チャンネル１３０との間に接続された内部通信インターフェイス２２５とを備えている。前記外部通信インターフェイス２１０および内部通信インターフェイス２２５は、前記外部コンピュータネットワーク１０５からダウンローダブルを受け取る機能、および、ダウンローダブルを前記内部コンピュータネットワーク１１５に送るための機能を有する統合的な通信インターフェイス(図示せず)の機能要素であってよい。

さらに、前記内部ネットワークセキュリティシステム１１０は、(キーボード、マウスおよびＣＲＴディスプレイなどの)入／出力(Ｉ／Ｏ)インターフェイス２１５と、磁気ディスクなどのデータ記憶装置２３０と、ランダムアクセスメモリ（ＲＡＭ）２３５とを備えており、これらの各々は前記信号バス２２０に接続されている。前記データ記憶装置２３０はセキュリティデータベース２４０を格納しており、該セキュリティデータベース２４０は、受け取ったダウンローダブルを疑わしいとすべきか否かを判定するためのセキュリティ情報を含んでいる。さらに、前記データ記憶装置２３０は、ダウンローダブルを受け取る可能性のある前記内部コンピュータネットワーク１１５内のユーザを示すユーザリスト２６０と、検査された各ダウンローダブルについての判定結果および前記内部ネットワークセキュリティシステム１１０の実行時表示を含むイベントログ２４５を格納している。オペレーティングシステム２５０は、前記ＣＰＵ２０５による処理を制御するものであり、典型的には前記データ記憶装置２３０に格納されており、（図示例では）前記ＲＡＭ２３５にロードされて実行される。セキュリティプ

ロ

グラム２５５は、入ってくるダウンローダブルの検査を制御するものであり、これも前記データ記憶装置２３０に格納されていて、（図示例では）前記ＲＡＭ２３５にロードされて前記ＣＰＵ２０５によって実行されてよい。

図３は、前記セキュリティプログラム２５５およびセキュリティデータベース２４０の詳細を示すブロック図である。前記セキュリティプログラム２５５は、ＩＤジェネレータ３１５と、該ＩＤジェネレータ３１５に接続されたポリシーファインダ３１７と、該ポリシーファインダ３１７に接続された第１のコンパレータ３２０とを含んでいる。前記第１のコンパレータ３２０は、４つの異なる経路、すなわち、経路１、経路２、経路３および経路４、を介して論理エンジン３３３に接続されている。前記経路１は、前記第１のコンパレータ３２０から前記論理エンジン３３３への直接的な接続部を含む。前記経路２は、前記第１のコンパレータ３２０に接続されたコードスキャナと、該コードスキャナ３２５を前記論理エンジン３３３に接続するアクセス・コントロール・リスト(ＡＣＬ)コンパレータ３３０とを含む。前記経路３は、前記第１のコンパレータ３２０に接続された証明書スキャナ３４０と、該証明書スキャナ３４０を前記論理エンジン３３３に接続する証明書コンパレータ３４５とを含む。前記経路４は、前記第１のコンパレータ３２０を前記論理エンジン３３３０に接続するユニフォーム・リソース・ロケータ(ＵＲＬ)を含む。また、記録エンジン３３５は、前記論理エンジン３３３と前記イベントログ２４５との間に接続されている。

前記セキュリティプログラム２５５は前記セキュリティデータベース２４０と協働して動作し、該セキュリティデータベース２４０は、セキュリティポリシー３０５と、既知のダウンローダブル３０７と、既知の証明書３０９と、前記既知のダウンローダブル３０７に対応したダウンローダブル・セキュリティ・プロファイル（ＤＳＰ）３１０を含む。前記セキュリティポリシー３０５は、特定のユーザ２６０に固有のポリシーと、入ってくるダウンローダブルを許可するへきかまたは拒絶するべきかを判定するためのデフォルト（または一般的）ポリシーとを含む。これらのセキュリティポリシー３０５は、拒絶すべき特定のダウンロー

ダブル、許可すべき特定のダウンローダブル、または、未知のダウンローダブルを許可するために必要な規準を指示することができる。図４において、前記セキュリティポリシー３０５は、ポリシーセレクタ４０５と、アクセスコントロールリスト４１０と、信頼性が確認された証明書リスト４１５と、ＵＲＬルールベース４２０と、管理オーバライドごとに許可または拒絶すべきダウンローダブルのリスト４２５とを含む。

前記既知のダウンローダブル３０７は、オリジナル機器マニュファクチャラ（ＯＥＭ）が悪意あるものとして認識しているダウンローダブルのリスト、および、このセキュリティプログラム２５５によって前に受け取られたダウンローダブルのリストを含む。前記ＤＳＰデータ３１０は、各前記既知のダウンローダブル３０７によって試みられる可能性のあるすべての潜在的に悪意のあるまたは疑わしいコンピュータオペレーションのリストを含むものであり、さらに、これらのそれぞれの引き数を含んでいてよい。オペレーションの確認された引き数は“確定された引き数”と称され、確認されていない引き数は“確定されていない引き数”と称される。次に、前記コードスキャナ３２５に関連して、前記ＤＳＰデータ３１０について説明する。

前記ＩＤジェネレータ３１５は、前記外部通信インターフェイス２１０を介して前記内部通信インターフェイス１０５からダウンローダブル（その送り元のＵＲＬおよび意図された受領者のユーザＩＤを含む）を受け取り、各ダウンローダブルを識別するためのダウンローダブルＩＤを生成する。該ダウンローダブルＩＤは、完全なダウンローダブルコードのディジタル・ハッシュ（hash）を含むのが好ましい。また、前記ＩＤジェネレータ３１５は、ダウンローダブルＩＤの生成のためのコードに含まれまたはこれによって識別されるすべての構成要素を前もってフェッチするのが好ましい。例えば、該ＩＤジェネレータ３１５は、ダウンローダブルＩＤの生成のためのJava（商標）アプレットのバイトコードに含まれまたはこれによって識別されるすべてのクラスを前もってフェッチしてよい。同様に、該ＩＤジェネレータ３１５は、ActiveX（商標）コントロールがダウンローダブルＩＤを算出するためのＩＮＦファイルにリストされたすべての構成要

素を取り出してよい。従って、ダウンローダブルのダウンローダブルＩＤは、前記ＩＤジェネレータ３１５が同一のダウンローダブルを受け取る時は常に同じものとなる。前記ＩＤジェネレータ３１５は、生成されたダウンローダブルＩＤを

前記既知のダウンローダブル３０７のリストに加える（それが未だリストされていない場合）。そして、前記ＩＤジェネレータ３１５は、前記ダウンローダブルおよびダウンローダブルＩＤを前記ポリシーファインダ３１７に送る。

前記ポリシーファインダ３１７は、意図されたユーザのユーザＩＤおよびダウンローダブルＩＤを使用して、受け取ったダウンローダブルに適用される特定のセキュリティポリシー３０５を選択する。前記ユーザ（またはそのスーパーグループの１つ）および前記ダウンローダブルについて定義された特定のポリシー３０５が存在する場合、そのポリシーが選択される。そうでない場合，前記ユーザ（またはそのスーパーグループの１つ）について定義された一般的なポリシー３０５が選択される。こうして、前記ポリシーファインダ３１７は、選択した前記ポリシーを前記第１のコンパレータ３２０に送る。

前記第１のコンパレータ３２０は、前記ポリシーファインダ３１７から、前記ダウンローダブル、ダウンローダブルＩＤおよびセキュリティポリシー３０５を受け取る。前記第１のコンパレータ３２０は、前記セキュリティポリシー３０５を検査し、前記ダウンローダブルを許可するためにどのステップが必要であるかを判定する。例えば、前記セキュリティポリシー３０５は、このダウンローダブルを許可するために、前記経路１、経路２、経路３および経路４からなる４つの経路のすべてを通らなければならない、ということを示してよい。代案として、前記セキュリティポリシー３０５は、このダウンローダブルを許可するために、前記経路のうちの１つだけを通らなければならない、ということを指示してよい。前記第１のコンパレータ３２０は、前記セキュリティポリシー３０５によって示された経路に適当な情報を送ることによって、これに応答する。

経路１

経路１において、前記第１のコンパレータ３２０は、前記ポリシーファインダ３１７から受け取ったセキュリティポリシー３０５のポリシーセレクタ４０５を

チェックする。該ポリシーセレクタ４０５が“許可された”または“拒絶された”ものである場合、前記第１のコンパレータ３２０は、この結果を直接前記論理エンジン３３３に送る。そうでない場合、前記第１のコンパレータ３２０は、ポリシーセレクタ４０５の内容に基づいて、経路２および／または経路３および／ま

たは経路４での比較を行う。なお、前記第１のコンパレータ３２０それ自体は、前記ダウンローダブルＩＤを、管理オーバライド４２５ごとに許可または拒絶するためのダウンローダブルのリストと比較する。すなわち、システムセキュリティアドミニストレータは、特定のダウンローダブルを“許可されるもの”または“拒絶されるもの”として定義することができる。

代案として、前記論理エンジン３３３が、各前記経路の結果を受け取り、前記ポリシーセレクタ４０５に基づき、前記ダウンローダブルを許可すべきか、または、拒絶すべきかを最終的に判定するようにしてもよい。前記第１のコンパレータ３２０は、その比較結果を前記論理エンジン３３３に通知する。

経路２

経路２において、前記第１のコンパレータ３２０は、前記ダウンローダブル、ダウンローダブルＩＤおよびセキュリティポリシー３０５を前記コードスキャナ３２５に送る。前記受け取ったダウンローダブルのＤＳＰデータ３１０が既知のものである場合、前記コードスキャナ３２５は、その情報を読み出し、前記ＡＣＬコンパレータ３３０に送る。そうでない場合、前記コードスキャナ３２５は前記ＤＳＰデータ３１０を分解する。すなわち、前記コードスキャナ３２５は、通常の解析技術を使用して、前記ダウンローダブルのコード（予めフェッチされたすべての構成要素を含む）をＤＳＰデータ３１０に分解する。該ＤＳＰデータ３１０は、特定のダウンローダブル３０７によって試みられる可能性のあるすべての潜在的に悪意のあるまたは疑わしいコンピュータオペレーションのリストを含むものであり、さらに、これらのオペレーションの各々の引き数を含んでよい。例えば、ＤＳＰデータ３１０は、特定のファイルからのREAD、未分解のホストへのSEND等を含んでいてよい。前記コードスキャナ３２５は、今まで潜在的に悪意

のあるものと判断され得たダウンローダブルコードにおけるすべてのオペレーションのリスト、および、前記ダウンローダブルコードによってアクセスされるすべてのファイルのリストとして前記ＤＳＰデータ３１０を生成することができる。なお、前記コードスキャナ３２５は、前記コードにおける、望ましくないまたは該コードがハッカによって書かれたことを示唆するパターンをサーチすることができる。

潜在的に悪意のあるものとして判断されるオペレーションのリストの例

ファイルオペレーション：ファイルのREAD（読み出し）、ファイルのWRITE（書き込み）；

ネットワークオペレーション：ソケットによるLISTEN（聞き取り）、ソケットへのCONNECT（接続）、データのSEND（送出）、データのRECEIVE（受取り）、VIEW INTRANET(イントラネット視察）；

登録オペレーション：登録アイテムのREAD（読み出し）、登録アイテムのWRITE（書き込み）；

オペレーティングシステムオペレーション：EXIT WINDOW(ウィンドウ退出)、EXIT BROWSER(ブラウザ退出)、START PROCESS/THREAD(オペレーション／スレッドの開始)、KILL PROCESS/THREAD(オペレーション／スレッドの停止)、CHANGE PROCESS/THREAD PRIORITY(オペレーション／スレッドの優先順位の変更)、DYNAMICALLY LOAD A CLASS/LIBRARY(クラス／ライブラリの動的ロード)など；

資源使用しきい値：メモリ、ＣＰＵ、グラフフィックスなど。

好ましい実施の形態において、前記コードスキャナ３２５は全内容検査を実行する。しかしながら、セキュリティの低減を伴うが速度を高める目的で、前記コードスキャナ３２５は、前記ダウンローダブルのヘッダのような一部分のみを検査してもよい。そして、該コードスキャナ３２５は、そのＤＳＰデータを（そのダウンローダブルＩＤに対応する）ＤＳＰデータ３１０に格納し、前記セキュリティポリシー３０５との比較のために、前記ダウンローダブルおよびＤＳＰデータを前記ＡＣＬコンパレータ３３０に送る。

該ＡＣＬコンパレータ３３０は、前記コードスキャナ３２５から前記ダウンロ

ーダブル、これに対応するＤＳＰデータおよびセキュリティポリシー３０５を受け取り、前記ＤＳＰデータをセキュリティポリシー３０５と比較する。すなわち、前記ＡＣＬコンパレータ３３０は、受け取ったダウンローダブルのＤＳＰデータを、受け取ったセキュリティポリシー３０５におけるアクセスコントロールリスト４１０と比較する。該アクセスコントロールリスト４１０は、前記ダウンローダブルを通すべきか、または、阻止すべきかを示す規準を含む。例えば、アクセスコントロールリストは、前記ＤＳＰデータがシステムファイルへのWRITEコマンドを含む場合に該ダウンローダブルが阻止されるべきものと示してよい。前記ＡＣＬコンパレータ３３０は、その結果を前記論理エンジン３３３に送る。

経路３

経路３において、前記証明書スキャナ３４０は、前記受け取ったダウンローダブルがVer is ign, Inc .のような証明書発行者によって署名されているか否かを判定し、該ダウンローダブルに含まれる証明書をスキャンする。前記証明書スキャナ３４０は、検出された証明書を前記証明書コンパレータ３４５に送る。該証明書コンパレータ３４５は、セキュリティアドミニスタレータによって信頼できるものと判断された既知の証明書を読み出し、前記検出された証明書を該既知の証明書と比較し、前記ダウンローダブルが信頼性のおける証明書によって署名されたものか否かを判定する。該証明書コンパレータ３４５は、その結果を前記論理エンジン３３３に送る。

経路４

経路４において、前記ＵＲＬコンパレータ３５０は、前記ダウンローダブルのソースを示すＵＲＬをＵＲＬルールベース４２０に格納されたＵＲＬに対して検査し、前記ダウンローダブルが信頼性のおけるソースから送られたものか否かを判定する。前記セキュリティポリシー３０５に基づき、前記ＵＲＬコンパレータ３５０は、前記ダウンローダブルが信頼のおけないソースから送られたもの、すなわち、信頼のおけるソースから送られたものではない場合に、該ダウンローダブルを疑わしいものと判断してよい。例えば、前記ダウンローダブルが既知のハッカから送られたものである場合、該ダウンローダブルは、疑わしいものと判断

され、悪意のあるものと推定されてよい。前記ＵＲＬコンパレータ３５０は、その結果を前記論理エンジン３３３に送る。

前記論理エンジン３３３は、各前記経路の結果および前記セキュリティポリシー３０５におけるポリシーセレクタ４０５を検査し、前記ダウンローダブルを許可すべき、または、拒絶すべきかを判定する。前記ポリシーセレクタ４０５は、各前記経路から受け取った論理表現を含む。例えば、該ダウンローダブルが前記経路のうちのいずれかで阻止された場合、すなわち、該ダウンローダブルが悪意のあるものである場合（経路１）、該ダウンローダブルが疑わしいオペレーションを要求する可能性のあるものである場合（経路２）、該ダウンローダブルが信頼性が確認された証明書発行者によって署名されていないものである場合（経路３）、または、該ダウンローダブルが信頼のおけないソースから送られたものである場合（経路４）に、前記論理エンジン３３３はこのダウンローダブルを拒絶することができる。前記論理エンジン３３３は、前記セキュリティポリシー３０５に含まれるポリシーセレクタ４０５に従って、他の論理表現を適用してよい。前記ダウンローダブルが通過可能であると前記ポリシーセレクタ４０５が示す場合、前記論理エンジン３３３は、該ダウンローダブルを意図された受領者に送る。前記ダウンローダブルが拒絶すべきものと前記ポリシーセレクタ４０５が示す場合、前記論理エンジン３３３は、悪意のないダウンローダブルを意図された受領者に送り、これにより、前記内部ネットワークセキュリティシステム１１０が前記オリジナルのダウンローダブルを放棄した旨ユーザに通知する。さらに、前記論理エンジン３３３は前記記録エンジン３３５にステータスレポートを送り、該記録エンジン３３５は、例えばＭＩＳディレクタによるその後の再検査のために、前記レポートをデータ記憶装置２３０のイベントログ２４５に格納する。

図５はセキュリティ管理コンソール１２０の詳細を示すブロック図であり、該セキュリティ管理コンソール１２０は、前記通信チャンネル１３５に接続されたセキュリティポリシーエディタ５０５と、前記通信チャンネル１３５とユーザ通知エンジン５１５との間に接続されたイベントログ分析エンジン５１０と、前記通信チャンネル１３５に接続されたダウンローダブルデータベース検査エンジン

５２０とを具備している。さらに、前記セキュリティ管理コンソール１２０は、図２に示されたコンピュータ構成要素と同様なコンピュータ構成要素を備えている。

前記セキュリティポリシーエディタ５０５は、Ｉ／Ｏインターフェイス２１５と同様なＩ／Ｏインターフェイスを使用して、前記セキュリティポリシー３０５の許可されたユーザ修正を可能にする。すなわち、前記セキュリティポリシーエディタ５０５は、許可されたユーザが、ユーザ２６０に対応する特定のセキュリティポリシー３０５、デフォルトまたは一般的なセキュリティポリシー３０５、

管理オーバライドごとに拒絶すべきダウンローダブル、管理オーバライドごとに許可すべきダウンローダブル、信頼性が確認された証明書のリスト４１５、ポリシーセレクタ４０５、アクセスコントロールリスト４１０、ＵＲＬルールベース４２０におけるＵＲＬなどを修正することを可能にする。例えば、許可されたユーザが新たな悪意のあるダウンローダブルについて知った場合、該ユーザは、システムオーバライドごとに拒絶すべきダウンローダブルに前記ダウンローダブルを加えることができる。

前記イベントログ分析エンジン５１０は、前記データ記憶装置２３０に格納されたイベントログ２４５に含まれるステータスレポートを検査する。該イベントログ分析エンジン５１０は、（例えば、セキュリティシステムマネージャまたはＭＩＳディレクタなどの）ユーザの通知が許可されたものか否かを判定する。例えば、３０分の期間内に内部ネットワークセキュリティシステム１１０によって１０個の疑わしいダウンローダブルが放棄された場合、前記イベントログ分析エンジン５１０は、ユーザ通知を許可し、これにより、潜在的な切迫したセキュリティ上の脅威を示してよい。従って、前記イベントログ分析エンジン５１０は、ユーザ通知エンジン５１５に対してユーザに通知するよう指示する。該ユーザ通知エンジン５１５は、内部通信インターフェイス２２０または外部通信インターフェイス２１０を介して、前記ユーザにｅメールを送ってよく、または、前記ユーザのディスプレイ装置（図示せず）にメッセージを表示してよい。

図６Ａは、疑わしいダウンローダブルから内部コンピュータネットワーク１１

５を保護するための方法６００を示すである。該方法６００は、前記ＩＤダウンローダブル３１５がダウンローダブルを受け取るステップ６０２から始まる。前記ＩＤダウンローダブル３１５は、ステップ６０４において、好ましくは、（予めフェッチされた構成要素を含む）ダウンローダブルコードのディジタルハッシュを生成することによって、受け取ったダウンローダブルを示すダウンローダブルＩＤを生成する。ステップ６０６において、前記ポリシーファインダ３１７は、意図された受領者（または、該意図された受領者が属するグループ）を示すユーザＩＤおよびダウンローダブルに対応する適当なセキュリティポリシー３０５を検出する。この選択されるセキュリティポリシー３０５は、デフォルトセキュリ

ティポリシー３０５であってよい。次に、図６Ｂを参照して、ステップ６０６についてより詳細に説明する。

ステップ６０８において、前記第１のコンパレータ３２０は、管理オーバライド４２５ごとに許可または拒絶すべきダウンローダブルのリストを入ってくるダウンローダブルのダウンローダブルＩＤに対して検査し、該ダウンローダブルを自動的に許可すべきか否かを判定する。許可すべき場合、ステップ６１２において、前記第１のコンパレータ３２０は、その結果を前記論理エンジン３３３に送る。許可すべきでない場合、前記方法６００はステップ６１０に進む。ステップ６１０において、前記第１のコンパレータ３２０は、管理オーバライド４２５ごとに拒絶すべきダウンローダブルのリストを入ってくるダウンローダブルのダウンローダブルＩＤに対して検査し、該ダウンローダブルを自動的に拒絶すべきか否かを判定する。拒絶すべき場合、ステップ６１２において、前記第１のコンパレータ４２０は、その結果を前記論理エンジン３３３に送る。拒絶すべきでない場合、前記方法６００はステップ６１４に進む。

ステップ６１４において、前記第１のコンパレータ３２０は、前記ダウンローダブルが経路４に従ってテストされるべき旨前記セキュリティポリシー３０５によって示されているか否かを判定する。ＮＯである場合、前記方法６００はステップ６１８にジャンプする。ＹＥＳである場合、前記ＵＲＬコンパレータ３５０

は、ステップ６１６において、前記入ってくるダウンローダブルに含まれたＵＲＬを前記ＵＲＬルールベース４２０と比較し、そして、前記方法６００はステップ６１８に進む。

ステップ６１８において、前記第１のコンパレータ３２０は、前記ダウンローダブルが経路２に従ってテストされるべき旨前記セキュリティポリシー３０５によって示されているか否かを判定する。ＮＯである場合、前記方法６００はステップ６２０にジャンプする。ＹＥＳである場合、ステップ６２６において、前記コードスキャナ２３５は、前記入ってくるダウンローダブルのダウンローダブルＩＤに基づいてＤＳＰデータ３１０を検査し、該ダウンローダブルが予め分解されたものか否かを判定する。ＹＥＳである場合、前記方法６００はステップ６３０にジャンプする。そうでなければ、ステップ６２８において、前記コードスキャナ２３５は、前記ダウンローダブルをＤＳＰデータに分解する。ダウンローダブル分解は図７を参照してより詳細に説明される。ステップ６３０では、ＡＣＬコンパレータ３３０が、入ってくるダウンローダブルのＤＳＰデータを、アクセスコントロールリスト４１０（これはダウンローダブルがテストに通るか落ちるかに必要な基準を含む）に対して比較する。

ステップ６２０において、前記第１のコンパレータ３２０は、前記ダウンローダブルが前記経路３に従ってテストされるべき旨前記セキュリティポリシー３０５によって示されているか否かを判定する。ＮＯである場合、前記方法６００は、テップ６１２に戻り、実行された各テストの結果を前記論理エンジン３３３に送る。ＹＥＳである場合、ステップ６２２において、前記証明書スキャナ６２２は、前記ダウンローダブルをスキャンし、そこに含まれる証明書をスキャンする。ステップ６２４において、前記証明書コンパレータ３４５は、信頼性が確認された証明書リスト（ＴＣＬ）４１５から信頼性が確認された証明書を読み出し、前記ダウンローダブルに含まれる証明書を前記信頼性が確認された証明書と比較し、前記ダウンローダブルが信頼性が確認されたソースによって署名されたものであるか否かを判定する。そして、、前記証明書コンパレータ３４５が各前記経路の結果を前記論理エンジン３３３に送ることによって、前記方法６００はステ

ップ６１２に進む。前記論理エンジン３３３のオペレーションについて、図６Ｃを参照して以下に詳しく説明する。そして、前記方法６００は終了する。

当業者に認識され得るように、前記テストは様々異なる順序で実行されてよく、各前記テストが実行されなくてもよい。さらに、当業者に認識され得るように、前記経路１は図６Ａにおいて自動許可または拒絶オペレーションとして説明したが、該経路１の結果は前記論理エンジン３３３によって適用される他の述語であってもよい。さらに、前記テストは図６Ａにおいて直列的に示されているが、これらのテストは図３に示したように並列的に実行されてもよい。

図６Ｂは、図６Ａのステップ６０６（以下、方法６０６という）の詳細を示すフローチャートである。この方法６０６によると、先ずステップ６５０において、前記ポリシーファインダ３１７は、前記セキュリティポリシー３０５がユーザＩＤおよびダウンローダブルに対応する特定のセキュリティポリシーを含むか否か

を判定する。ＹＥＳである場合、前記ポリシーファインダ３１７は、ステップ６５４において、前記対応するセキュリティポリシー３０５をフェッチする。ＮＯである場合、前記ポリシーファインダ３１７は、ステップ６５２において、前記ユーザＩＤに対応するデフォルトまたは一般的セキュリティポリシー３０５をフェッチする。そして、前記方法６０６が終了する。

図６Ｃは、前記入ってくるダウンローダブルを許可すべきか拒絶すべきかを判定するための方法６５５の詳細を示すフローチャートである。この方法６５５によると、先ずステップ６６０において、前記論理エンジン３３３は、前記第１のコンパレータ３２０、ＡＣＬコンパレータ３３０、証明書コンパレータ３４５およびＵＲＬコンパレータ３５０からそれぞれの結果を受け取る。前記論理エンジン３３３は、ステップ６６２において、前記結果を前記セキュリティポリシー３０５に含まれるポリシーセレクタ４０５と比較し、ステップ６６４において、前記ポリシーセレクタ４０５がダウンローダブルの通過を確認するか否かを判定する。例えば、前記ダウンローダブルが経路１～４のテストのうちの１つを通過する場合、前記論理エンジン３３３が該ダウンローダブルを通す旨前記ポリシーセ

レクタ４０５によって示されてよい。前記ダウンローダブルが通過すべき旨前記ポリシーセレクタ４０５が示す場合、前記論理エンジン３３３は、ステップ６６６において、前記ダウンローダブルを意図された受領者に送る。ステップ６６８において、前記論理エンジン３３３はその結果を前記記録エンジン３３５に送り、該記録エンジン３３５は、その後の再検査のために前記結果を前記イベントログ２４５に格納する。そして、方法６５５が終了する。ステップ６４４において前記ダウンローダブルが通過すべきでない旨前記ポリシーセレクタ４０５が示した場合、前記論理エンジン３３３は、ステップ６７０において前記ダウンローダブルを停止させ、そしてステップ６７２において、前記入ってくるダウンローダブルが阻止されたことをユーザに知らせるために悪意のない代替ダウンローダブルを送る。

図７は、ダウンローダブルをＤＳＰデータ３１０に分解するための図６Ａのステップ６２８（以下、方法６２８という）の詳細を示すフローチャートである。この方法６２８によると、先ずステップ７０５において、前記コードスキャナ３２５は前記ダウンローダブルのマシーンコードをディアセンブルする。前記コードスキャナ３２５は、ステップ７１０において前記マシーンコードにおけるそれぞれのコマンドを分解し、ステップ７１５において、前記分解されたコマンドが疑わしいものか否か(すなわち、前記コマンドが図３を参照して上述したリストに示されたオペレーションのうちの１つか否か)を判定する。ＮＯである場合、ステップ７２５において、前記コードスキャナ３２５は、前記ダウンローダブルの分解を完了したか否か、すなわち、前記ダウンローダブルコードにおけるすべてのオペレーションが分解されたか否かを判定する。ＹＥＳである場合、この方法６２８が終了する。ＮＯの場合、この方法６２８はステップ７１０に戻る。

前記コードスキャナ３２５は、ステップ７１５において前記分解された構成要素が疑わしいものであると判定した場合、ステップ７２０において前記疑わしいコマンドおよびそのコマンドパラメータをデコードして、ＤＳＰデータとして登録する。ステップ７２０において、前記コードスキャナ３２５は、前記コマンドおよびコマンドパラメータをコマンドクラス(例えば、ファイルオペレーション

、ネットワークオペレーション、登録オペレーション、オペレーティングシステムオペレーション、資源使用しきい値)に基づくフォーマットで登録する。そして、この方法６２８はステップ７２５にジャンプする。

図８は、ダウンローダブルを識別するためのダウンローダブルＩＤを生成するための方法８００を示すフローチャートである。該方法８００によると、先ずステップ８１０において、前記ＩＤジェネレータ３１５は、前記外部通信ネットワーク１０５からダウンローダブルを受け取る。前記ＩＤジェネレータ３１５は、ステップ８２０において、前記ダウンローダブルコードにおいて参照される構成要素のいくつかまたはすべてをフェッチしてよく、ステップ８３０において該フェッチされた構成要素を前記ダウンローダブルコードに含ませる。ステップ８４０において、前記ＩＤジェネレータ３１５は、前記ダウンローダブルコードの少なくとも一部についてハッシングファンクション（hashing function；ハッシング関数）を実行することにより、ダウンローダブルＩＤを生成する。ステップ８５０において、前記ＩＤジェネレータ３１５は、生成された前記ダウンローダブルＩＤをＤＳＰデータ３１０に対する参照としてセキュリティデータベース２４０に格納する。従って、前記ダウンローダブルＩＤは、同一のダウンローダブルに遭遇するごとに同じものとなる。

この発明は、上述の好ましい実施の形態に限定されることなく、様々な変更が可能である。例えば、この発明は内部コンピュータネットワークを保護するためのシステムとして説明したが、この発明は，個々のコンピュータを保護するためのシステムとして実施してもよい。また、この発明の構成要素は、プログラム化された汎用のディジタルコンピュータを使用して、アプリケーションごとに固有の集積回路を使用して、または、相互接続された通常の構成要素および回路を使用して実現されてよい。ここで述べた実施例は、あくまでも説明の為のものであって、完全さや限定を意図しているものではない。多くの別形態と変形とが、前述の教示に照らして、可能である。

【図１】

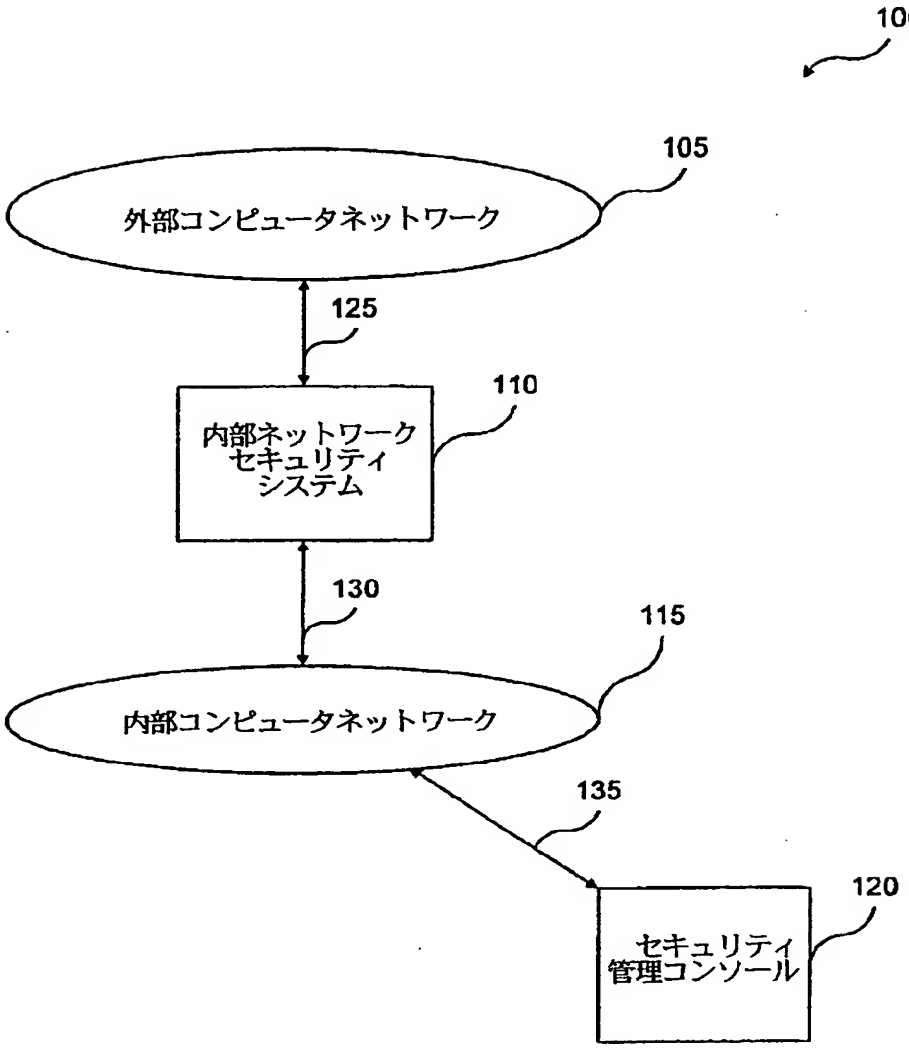
100
105
外部コンピュータネットワーク
125
110
内部ネットワーク
セキュリティ
システム
130
115
内部コンピュータネットワーク
135
120
セキュリティ
管理コンソール

図　1

【図２】

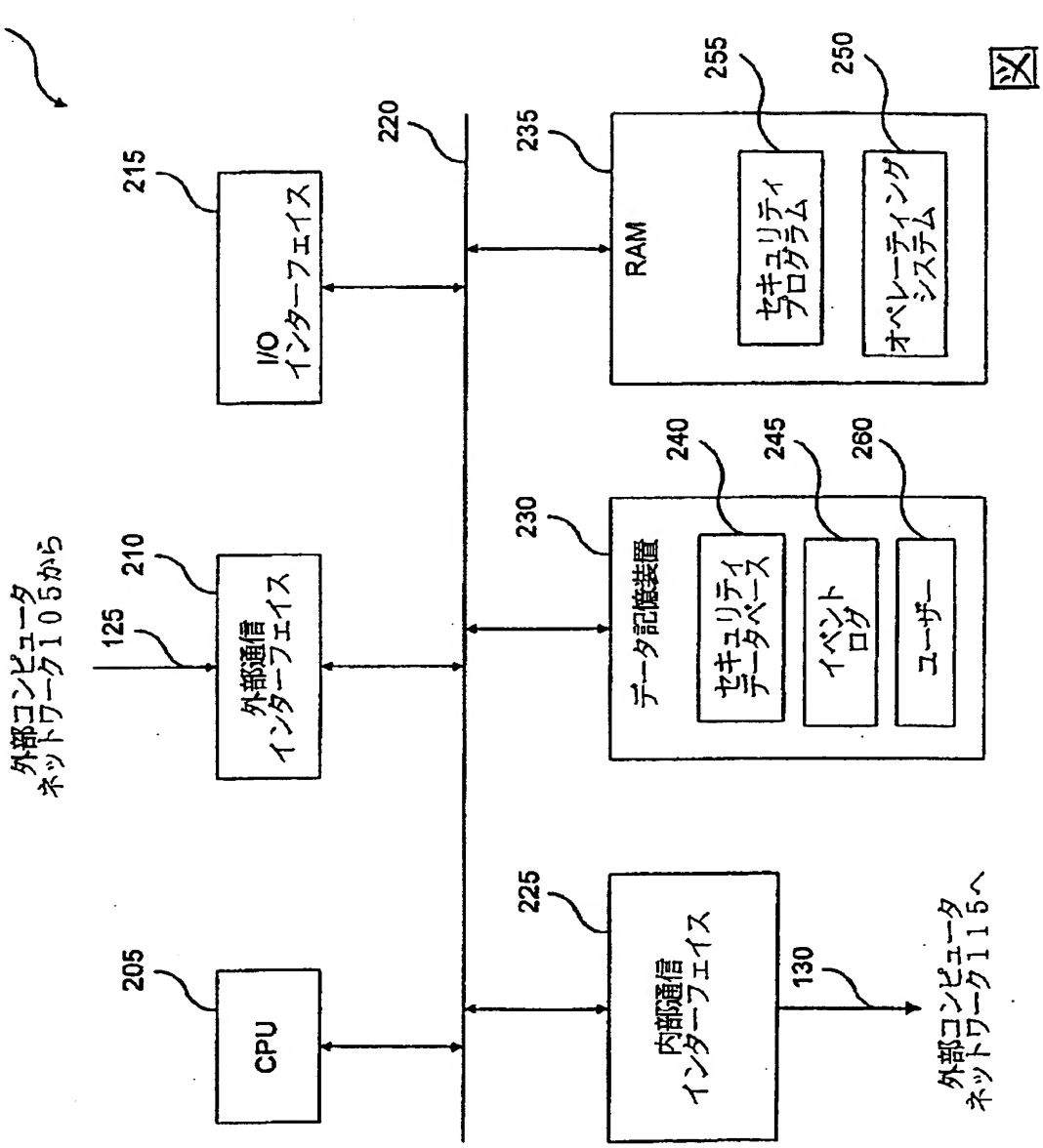
110
215
I/O
インターフェイス
220
235
RAM
255
セキュリティ
プログラム
250
オペレーティング
システム
外部コンピュータ
ネットワーク１０５から
125
210
外部通信
インターフェイス
230
データ記憶装置
240
セキュリティ
データベース
245
イベント
ログ
260
ユーザー
205
CPU
225
内部通信
インターフェイス
130
外部コンピュータ
ネットワーク１１５へ

図２

【図３】

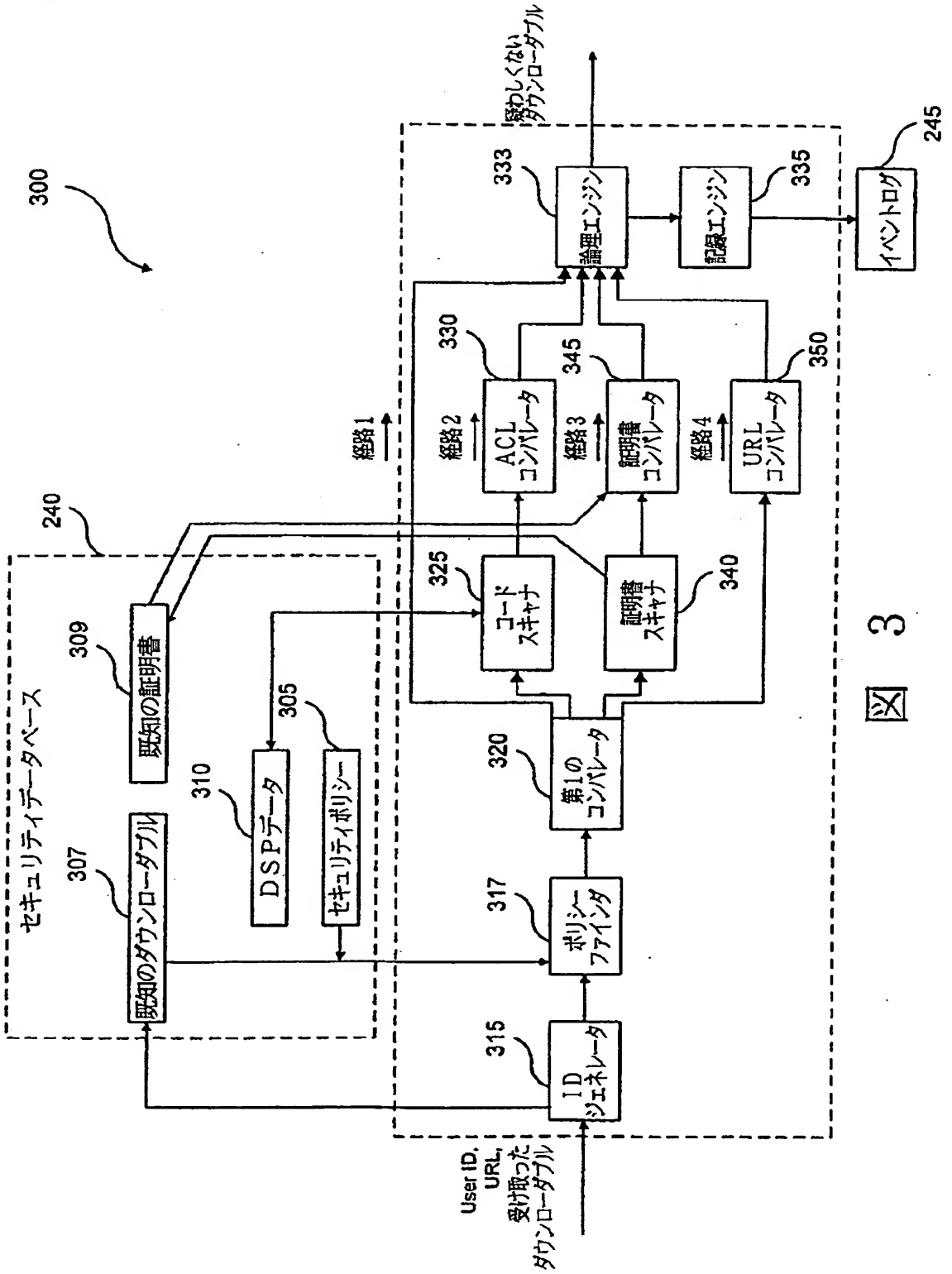
300
240
セキュリティデータベース
309
既知の証明書
307
既知のダウンローダブル
310
DSPデータ
305
セキュリティポリシー
315
IDジェネレータ
317
ポリシーファインダ
320
第1のコンパレータ
325
コードスキャナ
340
証明書スキャナ
330
ACLコンパレータ
345
証明書コンパレータ
350
URLコンパレータ
経路1
経路2
経路3
経路4
333
論理エンジン
335
記録エンジン
245
イベントログ
疑わしくないダウンローダブル
User ID,
URL,
受け取った
ダウンローダブル

図３

【図４】

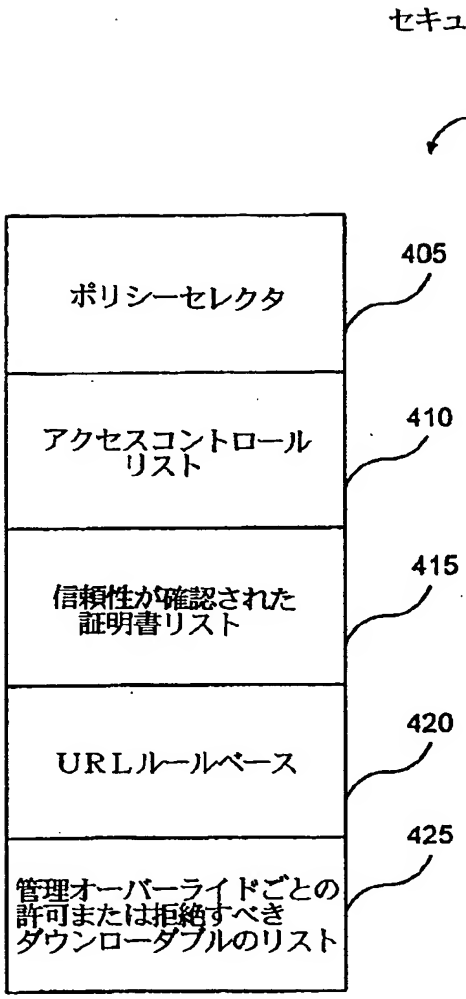
セキュリティポリシー
305
ポリシーセレクタ
405
アクセスコントロール
リスト
410
信頼性が確認された
証明書リスト
415
URLルールベース
420
管理オーバーライドごとの
許可または拒絶すべき
ダウンロードブルのリスト
425

図　４

【図５】

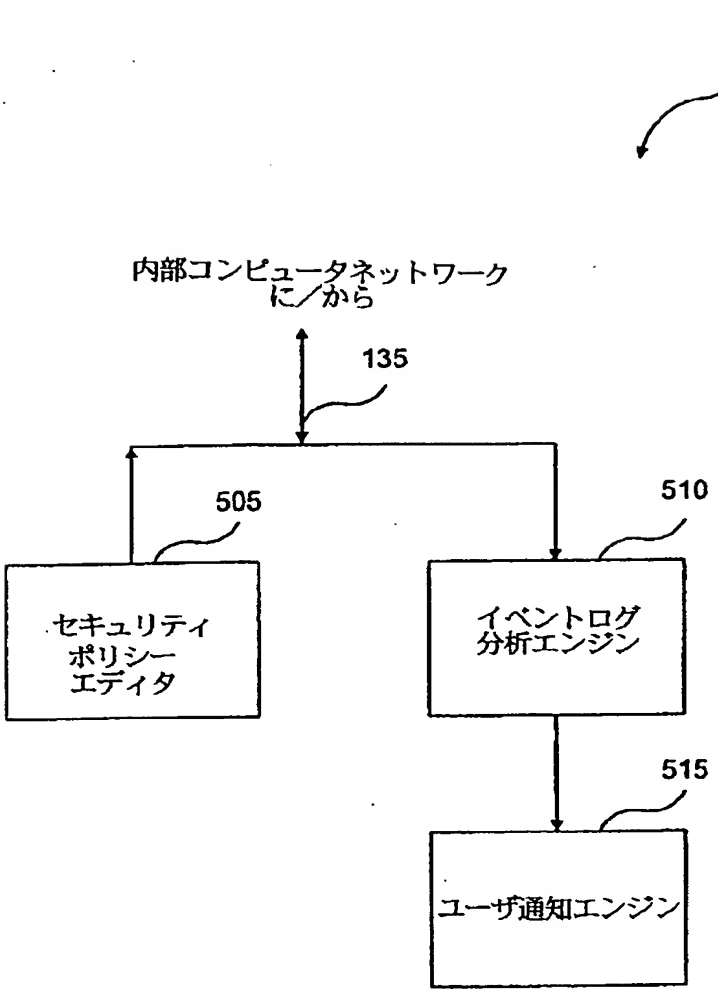
120
内部コンピュータネットワーク
に／から
135
505
510
セキュリティ
ポリシー
エディタ
イベントログ
分析エンジン
515
ユーザ通知エンジン

図　５

【図６】

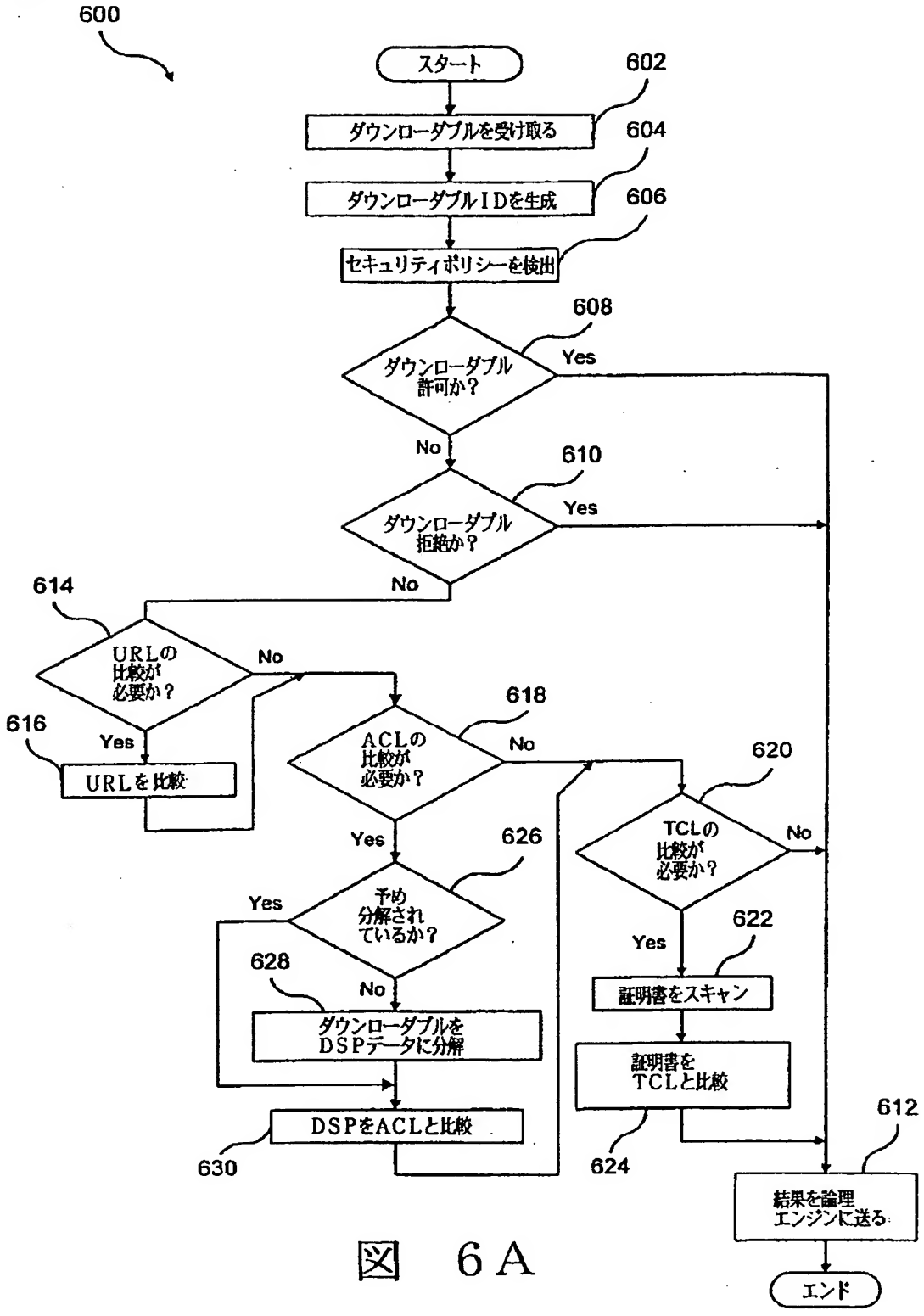
600
スタート
602
ダウンローダブルを受け取る
604
ダウンローダブルＩＤを生成
606
セキュリティポリシーを検出
608
ダウンローダブル許可か？
Yes
No
610
ダウンローダブル拒絶か？
Yes
No
614
URLの比較が必要か？
No
616
Yes
URLを比較
618
ACLの比較が必要か？
No
Yes
626
予め分解されているか？
Yes
628
No
ダウンローダブルをDSPデータに分解
DSPをACLと比較
630
620
TCLの比較が必要か？
No
Yes
622
証明書をスキャン
証明書をTCLと比較
624
612
結果を論理エンジンに送る
エンド

図 ６Ａ

【図６】

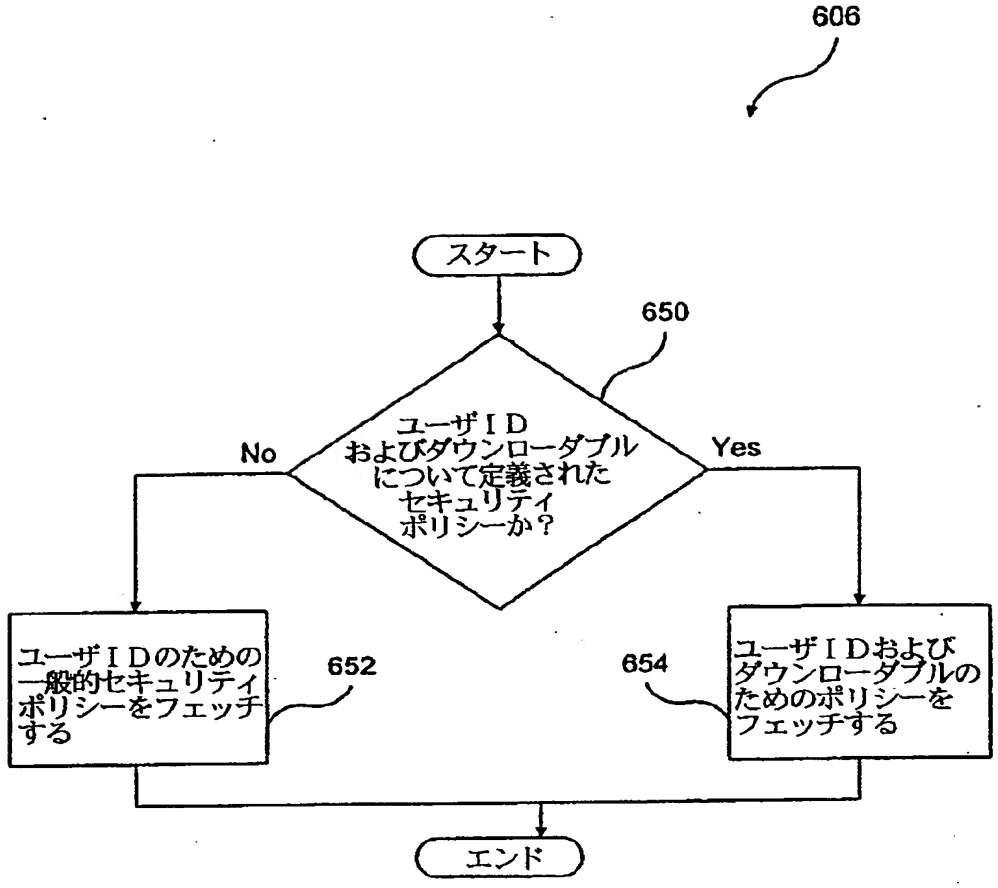
606
スタート
650
ユーザＩＤ
およびダウンローダブル
について定義された
セキュリティ
ポリシーか？
No
Yes
ユーザＩＤのための
一般的セキュリティ
ポリシーをフェッチ
する
652
654
ユーザＩＤおよび
ダウンローダブルの
ためのポリシーを
フェッチする
エンド

図　６Ｂ

【図６】

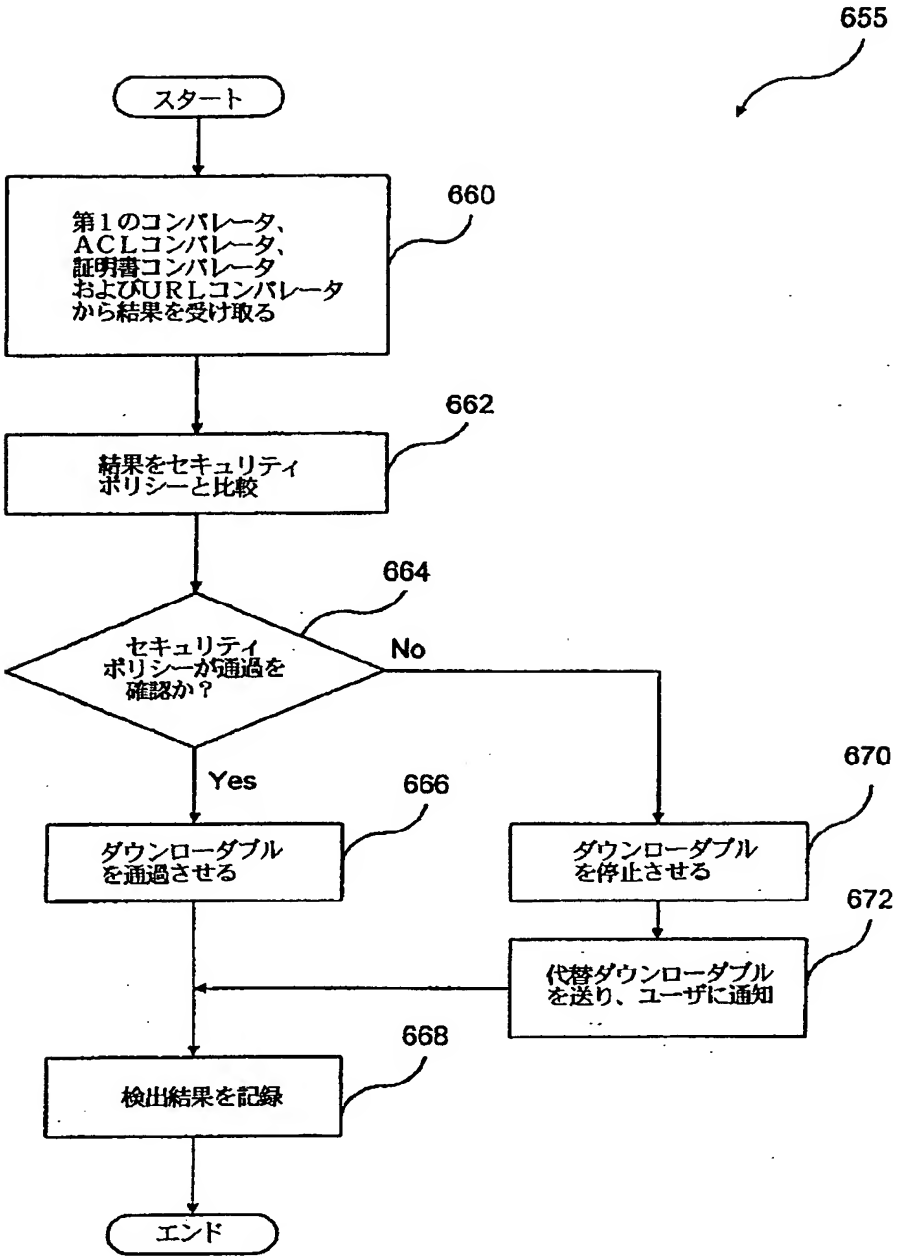
655
スタート
第１のコンパレータ、
ＡＣＬコンパレータ、
証明書コンパレータ
およびＵＲＬコンパレータ
から結果を受け取る
660
結果をセキュリティ
ポリシーと比較
662
セキュリティ
ポリシーが通過を
確認か？
664
No
Yes
ダウンロードブル
を通過させる
666
ダウンロードブル
を停止させる
670
代替ダウンロードブル
を送り、ユーザに通知
672
検出結果を記録
668
エンド

図 ６Ｃ

【図７】

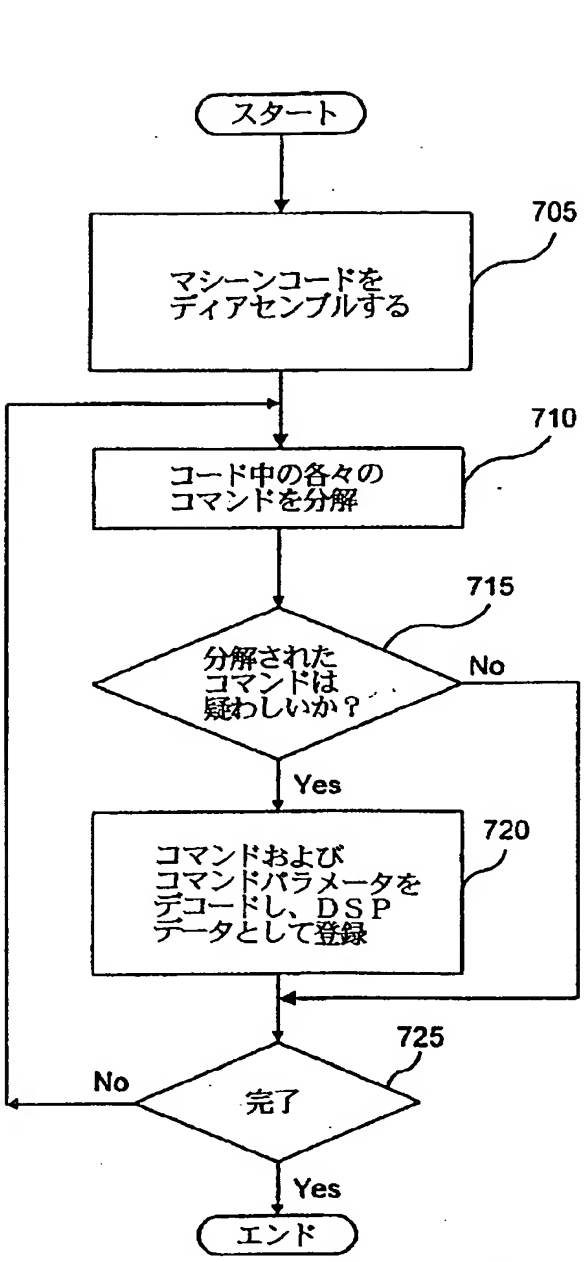
628
スタート
705
マシーンコードを
ディアセンブルする
710
コード中の各々の
コマンドを分解
715
分解された
コマンドは
疑わしいか？
No
Yes
720
コマンドおよび
コマンドパラメータを
デコードし、ＤＳＰ
データとして登録
725
No
完了
Yes
エンド

図　7

【図８】

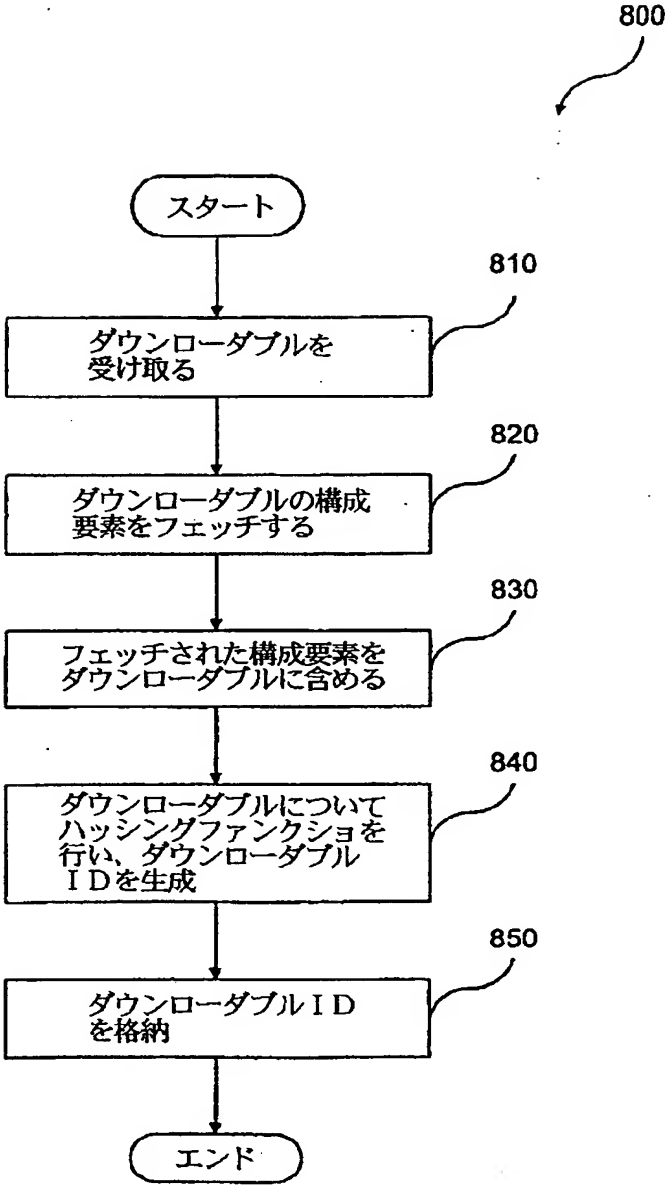
800
スタート
810
ダウンローダブルを
受け取る
820
ダウンローダブルの構成
要素をフェッチする
830
フェッチされた構成要素を
ダウンローダブルに含める
840
ダウンローダブルについて
ハッシングファンクションを
行い、ダウンローダブル
ＩＤを生成
850
ダウンローダブルＩＤ
を格納
エンド

図　８

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No.
PCT/IB97/01626

A. CLASSIFICATION OF SUBJECT MATTER
IPC(6) : G06F 19/00, 15/18, 9/44
US CL : 395/187.01, 186, 188.01, 200.48, 200.59, 10
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 395/187.01, 186, 188.01, 200.48, 200.59, 10

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

NONE

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

NONE

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X,P	US 5,572,643 A (JUDSON) 05 November 1996, col. 2, lines 12-53, col. 3, lines 48-67, col. 4, lines 5-51, col. 7, lines 1-13	1-70
X	US 5,077,677 A (MURPHY ET AL) 31 December 1991, COL. 2, LINES 60-66, COL. 19, LINES 8-16	10, 35
X,E	US 5,692,047 A (MCMANIS) 25 November 1997, col. 3, lines 14-29.	66

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

*	Special categories of cited documents:	"T"	later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A"	document defining the general state of the art which is not considered to be of particular relevance	"X"	document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E"	earlier document published on or after the international filing date	"Y"	document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L"	document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&"	document member of the same patent family
"O"	document referring to an oral disclosure, use, exhibition or other means		
"P"	document published prior to the international filing date but later than the priority date claimed		

Date of the actual completion of the international search 25 MARCH 1998	Date of mailing of the international search report 14 MAY 1998
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703) 305-3230	Authorized officer PIERRE EDDY ELISCA Telephone No. (703) 305-3987

Form PCT/ISA/210 (second sheet)(July 1992)*

フロントページの続き

(81)指定国 ＥＰ(ＡＴ，ＢＥ，ＣＨ，ＤＥ，ＤＫ，ＥＳ，ＦＩ，ＦＲ，ＧＢ，ＧＲ，ＩＥ，ＩＴ，ＬＵ，ＭＣ，ＮＬ，ＰＴ，ＳＥ)，ＣＡ，ＩＬ，ＪＰ

【要約の続き】
構成要素を含むダウンローダブルについてのハッシング関数を実行することによって、前記ダウンローダブルを識別するダウンローダブルＩＤを算出するためのＩＤジェネレータを使用する。前記セキュリティポリシーは、（１）既知の悪意のあるダウンローダブルおよび悪意の無いダウンローダブルとの比較、（２）管理オーバーライドごとの拒絶または許可すべきダウンローダブルとの比較、（３）ダウンローダブルセキュリティプロファイルデータの、アクセスコントロールリストに対する比較、（４）前記ダウンローダブルに含まれる証明書の、信頼性が確認された証明書との比較、（５）前記ダウンローダブルの送り元のＵＲＬの、信頼性が確認されたＵＲＬおよび信頼性が確認されていないＵＲＬに対する比較を含むいくつかの実行すべきテストを指示するものであってよい。これらのテストに基づき、論理エンジンは、前記ダウンローダブルを許可または拒絶すべきことを判定することができる。